EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 10142340
PUBLICATION DATE : 29-05-98

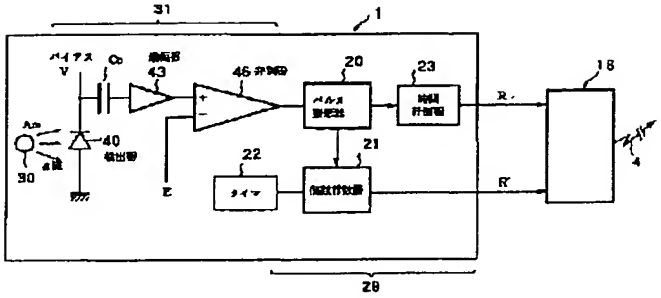
APPLICATION DATE : 08-11-96
APPLICATION NUMBER : 08296312

APPLICANT : TSUYUSAKI NORIHEI;

INVENTOR : TSUYUSAKI NORIHEI;

INT.CL. : G01T 1/17 G01T 1/30 G06F 7/58 G09C 1/00

TITLE : RANDOM NUMBER GENERATOR AND ENCRYPTION UNIT



ABSTRACT : PROBLEM TO BE SOLVED: To generate an undecodable encryption code by employing numeric values obtained by counting the discharging interval or number of faint radiation as natural random number.

SOLUTION: A shaped pulse signal is delivered from a pulse shaper 20 to a counter 21 which is set with a time interval (t) by a timer 22. The counter 21 counts the shaped pulse signals over the range of time interval (t) and outputs the count as a random number Rn. Shaped pulse signals from the pulse shaper 20 are also delivered to a time measuring unit 23 and the number of time pulses counted by the time measuring unit 23 before arrival of the shaped pulse is outputted as a random number Rt. An encryption unit 16 measures the radiation pulses discharged at random through natural decay directly and uses the number of measured pulses and the pulse interval, respectively, as random numbers R_n, R_t. Natural decay of a radioactive substance takes place at random and the time interval for discharging particles is determined and measured at random.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－142340

(43)公開日　平成10年(1998)５月29日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０１Ｔ	1/17		Ｇ０１Ｔ	1/17	Ｚ
	1/30			1/30	
Ｇ０６Ｆ	7/58		Ｇ０６Ｆ	7/58	Ｂ
Ｇ０９Ｃ	1/00	６５０	Ｇ０９Ｃ	1/00	６５０Ｂ

審査請求　未請求　請求項の数２　ＯＬ　（全６頁）

(21)出願番号　特願平8－296312

(22)出願日　平成８年(1996)11月８日

(71)出願人　595122279
露崎　知子
千葉県茂原市早野1820

(71)出願人　595122268
露崎　典平
千葉県茂原市早野1820

(72)発明者　露崎　典平
千葉県茂原市早野1820

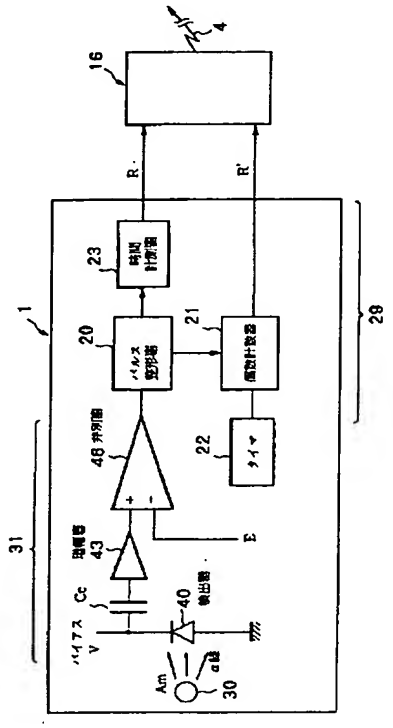
(74)代理人　弁理士　八嶋　敬市

(54)【発明の名称】　乱数発生装置と暗号化装置

(57)【要約】

【課題】　自然から乱数を抽出して、完全に近い乱数を得るとともに、この自然乱数により暗号化を行い解読不能な符号を生成する。

【解決手段】　所定の崩壊常数λに従い、時間ｔの経過とともに、放射線を放射して崩壊する微弱な放射性物質を使用し、この放射線の放出間隔を時間の関数として検出し、又は一定時間内の放射線の放出個数を計測し、この計数した数値を乱数として出力する計数回路とする。この乱数に対し特定の有意データを組み合わせて演算を行い暗号を生成する暗号生成回路とを備え、前記乱数とこの暗号データを電磁媒体あるいは光学媒体（赤外線等）を介して離れた位置にある情報処理装置に送り、この情報処理装置では解読回路により前記乱数とこの暗号データに逆演算を行い前記特定の有意データを再生する。



【特許請求の範囲】
【請求項1】　所定の崩壊常数λに従い、時間tの経過とともに、放射線を放射して崩壊する微弱な放射性物質を使用し、
この放射線の放出間隔を時間の関数として放射線の計数回路で検出し、又は一定時間内の放射線の放出個数を計数回路で計測し、この計数した数値を乱数として情報処理装置に送ることを特徴とする乱数発生装置。
【請求項2】　所定の崩壊常数λに従い、時間tの経過とともに、放射線を放射して崩壊する微弱な放射性物質を使用し、
この放射線の放出間隔を時間の関数として検出し、又は一定時間内の放射線の放出個数を計測しかつ、この計数した数値を乱数として出力する計数回路と、
この乱数に対し特定の有意データを組み合わせて演算を行い暗号を生成する暗号生成回路とを備え、
前記乱数とこの暗号データを電磁媒体あるいは光学媒体を介して離れた位置にある情報処理装置に送り、この情報処理装置では解読回路により前記乱数とこの暗号データとの間に逆演算を行い前記特定の有意データを再生することを特徴とする暗号化装置。
【発明の詳細な説明】
【0001】
【発明の属する分野】本発明は微弱な放射性物質を利用する乱数発生装置とその乱数を使用した暗号化装置及び個人認証システムに関する。
【0002】
【従来の技術】これまでの暗号化処理の手法は、ホワイトノイズ等を使用して数式処理を行い人工的に乱数を発生させていた。または、特開平8－123669号のように、混合合同法等の手法を使用して、決められた桁数を決められた回数回の加算や乗算、除算を計算機上で、暗号化処理をしていた。
【0003】これは、元になる乱数が人工的に作成されたものであり、また計算により生成されるため、高精度な乱数にならず、繰り返し使用しているうちに同じ関数になってしまい、映像化して観察すると、一定のパターンが規則的に発生するという欠点が知られている。（Ivars Peterso 「コンピューター・グラフィクスが開く現代数学ワンダーランド」奥田　晃訳　新曜社）
【0004】
【発明が解決しようとする課題】従来の乱数はコンピュータを使用し計算により生成するので、周期性の発生する域の乱数を使用して、決められた回数の符号化処理行うと、送信途上で盗聴された場合、現在のスピードの向上した計算機を持ってすれば、短時間に符号が解読されてしまう恐れがあった。本発明では、自然から乱数を抽出して、完全に近い乱数を得るとともに、この自然乱数により暗号化を行い解読不能な符号を生成することを目的にしている。
【0005】
【課題を解決するための手段】本発明の請求項1は、所定の崩壊常数λに従い、時間tの経過とともに、放射線を放射して崩壊する微弱な放射性物質を使用し、この放射線の放出間隔を時間の関数として放射線の計数回路で検出し、又は一定時間内の放射線の放出個数を計数回路で計測し、この計数した数値を乱数として情報処理装置に送る。請求項2は、所定の崩壊常数λに従い、時間tの経過とともに、放射線を放射して崩壊する微弱な放射性物質を使用し、この放射線の放出間隔を時間の関数として検出し、又は一定時間内の放射線の放出個数を計測し、この計数した数値を乱数として出力する計数回路と、この乱数に対し特定の有意データを組み合わせて演算を行い暗号を生成する暗号生成回路とを備え、前記乱数とこの暗号データを電磁媒体あるいは光学媒体（赤外線等）を介して離れた位置にある情報処理装置に送り、この情報処理装置では解読回路により前記乱数とこの暗号データに逆演算を行い前記特定の有意データを再生する。
【0006】
【発明の実施の形態】
実施の形態1．次に、本願の第1発明を図1、4、5、6に従って説明する。図6は本発明に係る放射線の自然崩壊による線源強度の減衰の原理を示す図である。天然または人工放射性物質の核種は、α、β、γ線等を放射して自然崩壊する、その際、各物質固有の所定の崩壊常数に従って崩壊する。相次で、放射されるα、β、γ線はランダムな時間間隔で検出される。今α線に注目して説明する。例えば、アメリシューム241（^{241}Am）では、α線（ヘリウム原子）がある単位時間にX個放出される（例えば100個／秒等）。しかしながら、ある単位時間にX個放出されるといっても、自然現象であるため、ある単位時間にY個放出される場合、Z個放出される場合、全然放出のない場合等があり、ただ長時間計測すれば、ある単位時間に所定個数放出されるという事実である。
【0007】ここで、ある単位時間に平均X個放出されるという捉え方を変更して、相次いで放出（検出）されるα線の時間間隔に注目し、先のα線から後のα線の放出までの時間の変量の確率的動き、つまり、確率分布をもって、放射の仕方を規定する。この時の時間の変量は各核種固有の所定の崩壊常数λに従って、常に一定の確率分布に従っていることが、経験則から知られている。このような確率分布は数学理論では到着理論に属し、放射時間間隔tのα線崩壊の様子は図6に示すような指数分布によって表される。
【0008】この指数分布を示す関数は式（1）のF（t）$=N_0\ e^{\{-\lambda t\}}$で表される関数である、以下{}内は指数を示し、N_0は初期原子数を示す。このλの崩壊常数は、アメリシューム（^{241}Am）の他にもデ

ータや公知の物理法則や実験技術により、現存する核種については完全に知られている。α線の放射を検出するには検出時間間隔を測定するよりもある時間帯に放射されるα線の個数を検出するのが簡単である。アメリシュームの崩壊はα線の放射時間間隔が指数関数Ｆに合うので、ある時間帯に放射されるα線の個数を検出すればよい。

【０００９】放射分布が指数分布を示す関数Ｆ（ｔ）＝N_0 ｅ｛－λｔ｝～（１）

に従う時、任意の時間ａにおける区間ｈ，（ａ，ａ＋ｈ）内に崩壊するα線の個数がｋ個である確率Ｐｋは、次の式（２）で表示できる。

Ｐｋ＝Ｍ｛ｋ｝ｅ｛－Ｍ｝／ｋ！～（２）

ここで｛｝内は指数を示し、Ｍは平均値を示し、ｋ！はｋの階乗である。この分布は図７のポアソン分布であり、時間区間の始点ａに無関係で、その平均値はＭである。

【００１０】本願発明者は原理を応用して、アメリシューム（^{241}Ａｍ）（放射性同位元素、以下単にＲＩと称す）の放射能による乱数を応用して乱数発生装置と暗号化装置を作成した。以下に上記原理による、乱数発生装置と暗号化装置について説明する。まず、図１は乱数発生装置（ＲＰＧ）１の構成を示し、乱数発生装置（ＲＰＧ）１は放射性カプセル３０と検出装置３１と乱数発生回路２９とから構成される。放射性カプセル３０は、人体に無害な微量のα、β、γ線を放射する、例えば人工の放射性核種（物質、以後ＲＩと称す）のアメリシューム241（^{241}Ａｍ）である。

【００１１】この放射性カプセル３０から放射されるα線は検出装置３１により検出される。この検出装置３１はＲＩからのα線等を検出し、検出信号を計測装置２９に出力する。検出装置３１は、ＲＩのα崩壊により放出されるα粒子をＰＩＮダイオードで電流として補足する公知の方法を利用する。

【００１２】乱数発生回路２９（計測装置）はこれら信号中から所定の放射能（αまたは、βまたは、γ線）による信号のみを選択し、かつ設定された所定の時間ｈ以内に計測される信号の個数を計数する。

【００１３】更に、検出装置３１はＰＩＮダイオード４０と結合コンデンサーＣｃ と前置増幅器４３と弁別器４６から構成されている。放射性カプセル３０にＰＩＮダイオード４０を対面させて、円筒形の金属筒内に納めて半導体内にα線源が侵入し易いようにした。

【００１４】バイアス電圧ＶがＰＩＮダイオード４０に印加され、ＰＩＮダイオード４０はｐ－ｎ結合の半導体であって、α線源が侵入すると不安定電子や不安定正ホールが移動し、いわゆる通電し、ＰＩＮダイオード４０の両端に電流が発生する。

【００１５】この変動電流は微弱なもので結合コンデンサーＣｃ を介して前置増幅器４３に送られ、そこで増幅され、パルス信号として出力される。弁別器４６には、これらパルス信号と基準電圧Ｅとが送られ、ノイズを分離するため基準電圧Ｅより大きいパルス及び基準内の信号のみを選択する。即ち、前置増幅器４３からはα線によるパルス信号と他の雑音によるパルス信号が混在しているので、弁別器４６により、α線によるパルス信号だけを取り出すようにしている。

【００１６】この乱数発生装置（ＲＰＧ）１では、基準電圧Ｅを適当に設定して、α線の放射線によるパルス信号のみを取り出すようにする。今ここではα線に注目して、α線を放出する ^{241}Ａｍ核種の場合について述べたが、β線、γ線についても同様に計測可能である。乱数発生回路２９は、パルス整形器２０と個数計数器２１とタイマ２２と時間計測器２３とから構成される。放射線によるパルス信号は、乱数発生回路２９のパルス整形器２０に送られ、以後の計数回路のパルス波計との標準化がなされる。

【００１７】パルス整形器２０からの整形済パルス信号は個数計数器２１に送られ、個数計数器２１にはタイマ２２から時間間隔ｔ が設定される。個数計数器２１では、図４に示すように設定された時間間隔範囲で整形済パルス信号を計数し、計数値を乱数Ｒｎ ：３，５，２，１・・として出力する。単位時間に計測された放射線のパルスのランダムな数値をそのまま乱数Ｒｎ として使用する。

【００１８】またパルス整形器２０からの整形済パルス信号は時間計測器２３に送られ、時間計測器２３では時間パルスを計数しているが、図５に示すように整形済パルス信号が到着する時間、時間パルスの数を乱数Ｒｔ ：８，５，７・・秒（例えば）として出力する。乱数発生装置（ＲＰＧ）１は、自然崩壊によるランダムに放出される放射線をパルスとして直接計測し、計測されたパルス間隔（時間）を乱数Ｒｔ として使用する。

【００１９】放射性物質（ＲＩ）の自然崩壊は全くランダムに起こる現象であり、放出される粒子の放出時間の間隔は全くランダムであり、よって計測される時間間隔も全くランダムとなる。今、設定された時間間隔範囲で計数された整形済パルス信号、即ち、単位時間に放射性物質の自然崩壊で計数される乱数Ｒｎ について考察する。

【００２０】線源の強度が弱い放射性物質（ＲＩ）の自然崩壊で計測される単位時間のα線数が、０＜Ｒｎ ＜５～６０の範囲の場合は、図７のポアソン分布になり、α線数が、Ｒｎ ＞５～６０の範囲の場合は、図８の左右対称のガウス分布になる。

【００２１】得られた計数される乱数Ｒｎ は、どちらの分布でも平均計数値Ｍを中心にした数値に分布するが、例えば平均計数値Ｍ＝７なら７が一番多く、６、８が次に、また５、９がその次に多く計数される。しかしこれら数７、６、８、５、９等の発生順は、全くランダムで

あり、計数値は乱数Rn として信頼できる。

【００２２】乱数発生装置（ＲＰＧ）１からの乱数Rtまたは乱数Rn は暗号化装置１６に送られ、そこで暗号の生成に利用される。さて、ＲＰＧ１では線源強度を調整することにより、平均的な放出時間を調整することは可能である。崩壊は人工的にコントロールすることは一切できない、よって得られた関数は、全くランダム関数である、人工的に作成されたものではない。

【００２３】計測時間、計測個数を８ビット、１６ビット、３２ビット、６４ビットの桁数と対応させて、ビットに対応する数値を乱数として使用できる。また各ビットに対応した０または１を計測するＲＰＧを設置してもよい、この場合は放射線を検出した時１、検出しなかった時０、とすれば線源強度は検出限界まで、低下させることができる。ランダムに得られる時間の数値、あるいは単位時間に計測されるパルスの数値をそのまま乱数として、使用する。

【００２４】次に、図２、３において、第２発明の暗号化装置１６を説明する。暗号化装置１６は、送信側は前述の乱数発生装置（ＲＰＧ）１と暗号生成回路２と規則決定部１０と演算種テーブル１３と送信回路３とから構成される。乱数発生装置（ＲＰＧ）１からの乱数Rは、規則決定部１０と暗号生成回路２に送られ、暗号生成回路２には特定の有意データＳも送られてくる。

【００２５】演算種テーブル１３は演算種を予め記憶し、規則決定部１０は乱数と有意データとの間でどのような演算を実行するのかを、乱数に基づき演算種テーブル１３を参照して暗号生成回路２に指定する。

【００２６】規則決定部１０は乱数発生装置（ＲＰＧ）１からの乱数Rに従い、演算種テーブル１３から、初期値が奇数なら加算、偶数なら減算、或は実数の０なら乗算、１なら除算、２なら自乗・・・等の演算種Ｚを読み出し、暗号生成回路２に指令する。

【００２７】暗号生成回路２では、この乱数Rに対し特定の有意データを、例えば加算し暗号信号ＲＳとして送信回路３に出力する。送信回路３には、乱数発生装置（ＲＰＧ）１からの乱数Rも送られており、送信回路３は、乱数Rとこの暗号データＲＳを混合信号Ｒ、ＲＳとして、電磁媒体の通信回線４や電波及び光学媒体（赤外線等）を介して離れた位置にある図３の情報処理装置８に送る。

【００２８】図３の受信側では、情報処理装置８は、分離回路５と解読回路６と情報処理部７と規則再現部１１と逆演算種テーブル１２とから構成される。通信回線４からの混合信号Ｒ、ＲＳは、分離回路５により乱数Rと暗号データＲＳとに分離され、分離された乱数Rとこの暗号データＲＳは解読回路６に別々に入力され、分離された乱数Rは規則再現部１１に送られる。

【００２９】逆演算種テーブル１２には、演算種テーブル１３の奇数なら加算、偶数なら減算、或は実数の０なら乗算、１なら除算、２なら自乗・・・等の演算種Ｚに対応して、逆演算種－Ｚの一覧を予め格納している。

【００３０】乱数Rは規則再現部１１に送られ、規則再現部１１は乱数Rの初期値を参照して、逆演算種テーブル１２から受信した演算種Ｚの逆演算種－Ｚを読み出し、解読回路６に送る。解読回路６では、逆演算種－Ｚに従い、暗号データＲＳから乱数Rを減算、逆演算を行い、特定の有意データＳを再生する。

【００３１】有意データＳは情報処理部７に送られ、電子取り引きや、株取り引き、セキュリティーコード、秘密情報の伝達等に利用される。さて、暗号化の各種方法について説明する。送信側では、乱数Ｒ７５３５４３７８の初期値、先頭が７（奇数）なら演算を規則１に決定。

【００３２】加算の場合：Ｒ＋Ｓ＝ＲＳ、規則１：各桁を加算するが桁上りはしない。

乱数Ｒ	７５３５４３７８	９３２４４８３１	４６３６７４８９	・・・
有意データＳ	１	２	３	・・・
暗号データＲＳ	７５３５４３７９	９３２４４８３３	４６３６７４８２	
混合信号Ｒ、ＲＳ	７５３５４３７８	７５３５４３７９		
	９３２４４８３１	９３２４４８３３		
	４６３６７４８９	４６３６７４８１		
	・・・	・・・		

【００３３】受信側　乱数Ｒ７５３５４３７８の先頭が７（奇数）だから規則１の逆算に決定。

暗号データＲＳ	７５３５４３７９	９３２４４８３３	４６３６７４８２
乱数Ｒ	－７５３５４３７８	９３２４４８３１	４６３６７４８９
有意データＳ（差）	１	２	３

注：４６３６７４８２－４６３６７４８９では、各桁は独立とし、不足したら、その桁にのみ１０を加えたものから引く、２－９では１０＋２－９＝３とする。

【００３４】加算の場合：Ｒ＋Ｓ＝ＲＳ、規則１：各桁

乱数Ｒ	４桁	３７２７	

減算の場合：ＲＳ－Ｒ＝Ｓ、規則２：各桁を減算するが上位桁から引かない。

暗号データＲＳ	７５３５４３７９	９３２４４８３３	４６３６７４８２
乱数Ｒ	－７５３５４３７８	９３２４４８３１	４６３６７４８９
有意データＳ（差）	１	２	３

を加算するが桁上りはしない。

送信側　乱数Ｒ３７２５の初期値、先頭が３（奇数）なら演算を規則１に決定。

有意データＳ　４桁
暗号データＲＳ４桁
混合信号Ｒ、ＲＳ　通信回路上のデータ

【００３５】受信側　乱数Ｒ３７２７の先頭が３（奇数）だから規則１の逆算に決定。

暗号データＲＳ
乱数Ｒ
有意データＳ（差）

注：７８０２－３７２７では、各桁は独立とし、不足したら、その桁にのみ１０を加えたものから引く、０－２では１０＋０－２＝８とする。

【００３６】この発明では、完全乱数でデータを暗号化し、かつ演算種テーブル１３（逆演算種テーブル１２）を乱数０、１、２、３、４、５、６、７、８、９や偶数、奇数等毎に、予め送信側と受信側で決定しておいて使い分けるので、データの都度演算種を自動発生することができ、完全な暗号に近くなり、第三者による盗聴や解読が不可能になる。

【図面の簡単な説明】

【図１】本発明の乱数発生装置の一実施例を示す回路のブロック図である。

【図２】本発明の暗号化装置の送信側の一実施例を示す回路のブロック図である。

【図３】本発明の暗号化装置の受信側の一実施例を示す回路のブロック図である。

【図４】単位時間に計測されるランダムパルスの数値を示す図である。

【図５】本発明の乱数発生装置からランダムに得られる時間値を示す図である。

【図６】本発明に利用する崩壊現象を示す指数関数の図である。

【図７】一般的なポアソン分布のグラフ図である。

【図８】一般的なガウス分布のグラフ図である。

【符号の説明】

１　乱数発生装置
２　暗号生成回路

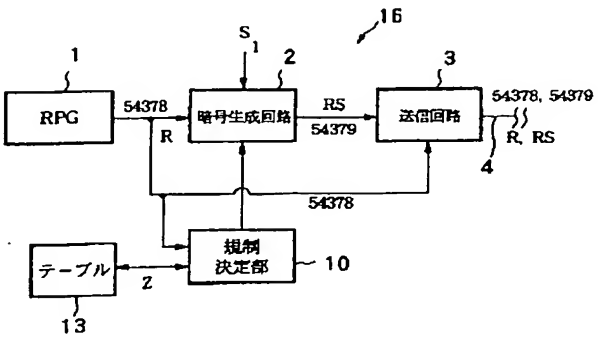
＋４１８５
　７８０２
３７２７　７８０２

減算の場合：ＲＳ－Ｒ＝Ｓ、規則２：各桁を減算するが上位桁から引かない。

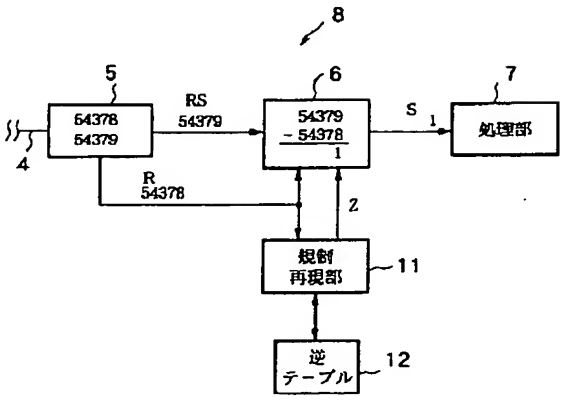
　７８０２
－３７２７
　４１８５

３　送信回路
４　通信回線
５　分離回路
６　解読回路
７　情報処理部
８　情報処理装置
１０　規則決定部
１１　規則再現部
１２　逆演算種テーブル
１３　演算種テーブル
１６　暗号化装置
２１　個数計数器
２２　タイマ
２３　時間計測器
２９　乱数発生回路
３０　放射性カプセル
３１　検出装置
３２　計測装置
４０　ＰＩＮダイオード
４３　前置増幅器
４６　弁別器
Ｃｃ　結合コンデンサー
Ｅ　基準電圧
Ｒ、ＲＳ　混合信号
Ｒ　乱数
ＲＳ　暗号データ
Ｓ　有意データ
Ｖ　バイアス電圧

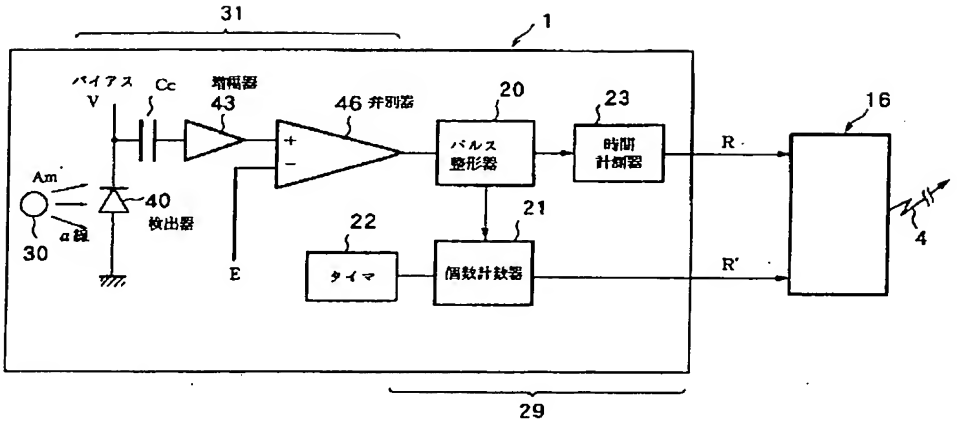
【図２】



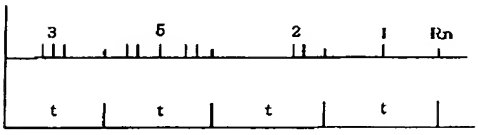
【図３】



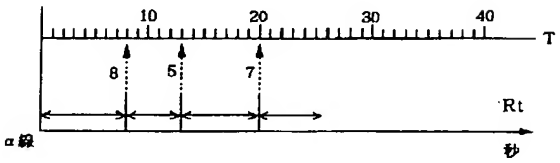
【図1】



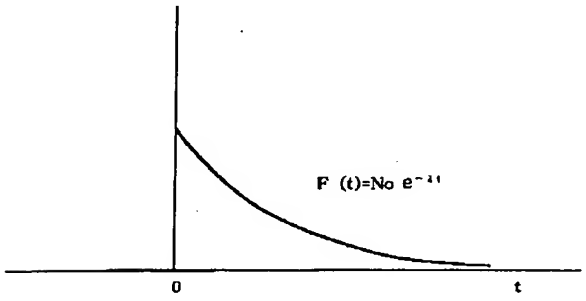
【図4】



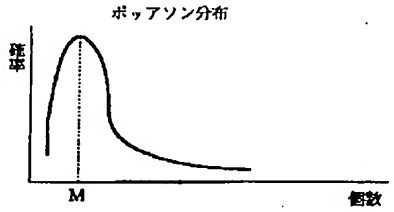
【図5】



【図6】



【図7】



【図8】